

Fabrice Mouhartem

CV



LIP, É.N.S. de Lyon,
46 allée d'Italie,
69364 Lyon Cedex 07
M +33 (0)6 38 61 92 22
E fabrice.mouhartem@ens-lyon.org
Nationality: French

Education

- PhD student**, L.I.P., É.N.S. de Lyon, France, Privacy-Preserving Cryptography from Pairings and Lattices.. **2015-now**
Advisor: Benoît Libert
- Master d'Informatique Fondamentale**, É.N.S. de Lyon, France, (university-level institution training teachers and researchers, entrance to which is based on a competitive exam. Equivalent to a Master of Science Degree in Computer Science). **2013-2015**
Cum Laude
- Licence d'Informatique Fondamentale**, É.N.S. de Lyon, France, (equivalent to a Bachelor of Science Degree in Computer Science). **2012-2013**
Cum Laude
- Classe préparatoire scientifique**, Lycée Charlemagne, Paris. **2010-2012**
(Post secondary preparatory class in science for competitive exam to the É.N.S.)
- Baccalauréat Scientifique**, Lycée d'Arsonval, Saint-Maur-des-fossés, Major : **2010**
Maths, Physics, Biology.
Cum laude

Experience

Research

- Supervision of a one week internship**, É.N.S. de Lyon, Lyon, France. **May 2016**
Make a ninth grade student intern discover fundamental research laboratories
- 5 Month Research Internship**, É.N.S. de Lyon, Lyon, France, Design a lattice-based dynamic group signature scheme. **Spring 2015**
- 3 Month Research Internship**, Katholieke Universiteit Leuven, Leuven, Belgium, Implementation in MAGMA of the state of the art *discrete logarithm* solving algorithm in small characteristic with improvements on them. **Summer 2014**
- 6 Week Research Internship**, Inria, Rennes, France, Works on the BARRA simulator to implement techniques to improve energy efficiency of GPUs using data redundancy. **Summer 2013**
Introduction to research.

Teaching

- Teaching Assistant**, É.N.S. de Lyon, Lyon, France. **2015-now**
- 2017-2018**
- Computer Architecture (L3). 32h
 - Project (LIFProjet) in *Université Claude Bernard Lyon 1*. 32h
- 2016-2017**
- Computational Complexity (M1). 20h
 - Cryptography and Security (M1). 20h
 - Operating Systems and Networks (L3). 32h
 - Jury for M1 thesis. 2h
- 2015-2016**
- Programming Language Theory (L3). 32h
 - Computational Complexity (M1). 20h
 - Remedial courses in Probability (L3). 2h

Oral examination, Lycée du Parc, Lyon, France, Oral exercises to post-secondary students to train them for competitive exams. 2013–2015

Administrative Responsibilities

Laboratory Council, LIP, É.N.S. de Lyon, Lyon. 2017–2018

PhD representative at the laboratory council of the LIP.

Scientific Council, É.N.S. de Lyon, Lyon. 2015–2017

Student representative at the scientific council of É.N.S. de Lyon.

Popularisation

Origami in Math and C.S., É.N.S. de Lyon/MMI, Lyon. April 2017

Open access origami workshop about mathematical origamis.

Origami in Math and C.S., É.N.S. de Lyon/MMI, Lyon. 2017

Organisation of a bimonthly origami's workshops.

Animator at Fête de la Science, É.N.S. de Lyon, Lyon. October 2015, 2016 & 2017

Organisation of a workshop about mathematical origamis.

Programming Contests

Qualified for the Google Hash Code Final, Google Dublin, Dublin, Ireland. March 2017

Team algorithmic/optimization competition, participation in C++, 12th out of ≥ 4500 participants.

Contestant for the ACM ICPC SWERC, Universidad do Porto, Porto, Portugal. November 2014 & 2015

Team algorithmic competition, participation in C++

Contestant for the ACM ICPC SWERC, Universitat de València, València, Spain. November 2013

Contestant for Prologin, EPITA, Paris, France. 2013

Individual algorithmic & A.I. competition, participation in C++

Publications

Conferences

Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Adaptive oblivious transfer with access control from lattice assumptions. In *Asiacrypt'17*, pages 533–563. Springer, 2017.

<https://hal.inria.fr/hal-01622197>.

Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions. In *Asiacrypt'16*, pages 373–403, 2016.

<https://ia.cr/2016/101>.

Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption. In *Asiacrypt'16*, pages 101–131, 2016.

<https://ia.cr/2016/879>.

Benoît Libert, Fabrice Mouhartem, and Khoa Nguyen. A Lattice-Based Group Signature Scheme with Message-Dependent Opening. In *ACNS'16*, pages 137–155. Springer, 2016.

<https://hal.inria.fr/hal-01302790>.

Benoît Libert, Fabrice Mouhartem, Thomas Peters, and Moti Yung. Practical “Signatures with Efficient Protocols” from Simple Assumptions. In *AsiaCCS'16*, pages 511–522. ACM, 2016.

<https://hal.inria.fr/hal-01303696>.

Talks

Conference talks

Asiacrypt, Hong Kong, China, 25 min. December 2017

Adaptive Oblivious Transfer with Access Control from Lattice Assumptions

- Asiacrypt**, Hanoi, Vietnam, 25 min. **December 2016**
Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions.
- ACNS**, University of Surrey, United Kingdom, 25 min. **June 2016**
A Lattice-Based Group Signature Scheme with Message-Dependent Opening.
- AsiaCCS**, Xi'an, China, 25 min. **June 2016**
Practical "Signatures with Efficient Protocols" from Simple Assumptions.

Seminars

- Department Seminar**, Indian Institute of Technology Madras, Chennai, India, 1h. **August 2018**
Privacy-Preserving Cryptography from Pairings and Lattices
- Talk at Microsoft Research**, Microsoft Research Bangalore, India, 1 hour. **July 2018**
Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption.
- AriC "back from conferences"**, É.N.S. de Lyon, France, 15 min. **May 2018**
Post-Quantum Fiat Shamir.
- Caen Crypto Seminar**, Caen, France, 1 hour. **November 2017**
Adaptive Oblivious Transfer with Access Control for NC^1 from LWE.
- Oxford Crypto Seminar**, Oxford, UK, 1 hour. **November 2017**
Adaptive Oblivious Transfer with Access Control from Lattice Assumptions.
- Rennes Crypto Seminar**, Rennes, France, 1 hour. **June 2017**
Adaptive Oblivious Transfer with Access Control for NC^1 from LWE.
- Journées du GT-C2**, Inria Nancy – Grand Est, La Bresse, 30 min. **April 2017**
Adaptive Oblivious Transfer with Access Control for Branching Programs.
- Lattice meeting**, É.N.S. de Lyon, France, 1h30. **April 2017**
Adaptive Oblivious Transfer from LWE.
- Caen Crypto Seminar**, Caen, France, 1 hour. **November 2016**
Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions.
- RAIM**, Banyuls-sur-Mer, France, 30 min. **June 2016**
Group Signatures and Lattice-Based Cryptography.
- AriC Crypto Fair**, É.N.S. de Lyon, France, 10 min. **June 2016**
Lattice-Based Group Encryption.
- Journées du GT-C2**, Université de Toulon, France, 25 min. **October 2015**
A Dynamic Group Signature Scheme based on Lattices.
- Lattice meeting**, É.N.S. de Lyon, France, 1h30. **October 2015**
Lattice-based group signature for dynamic groups.
- Séminaire AriC**, É.N.S. de Lyon, France, 1h. **September 2015**
Lattice-based dynamic group signature.

Popularisation

- Al-Kindi cryptography contest**, É.N.S. de Lyon, Lyon. **May 2018**
Overview of zero-knowledge proofs for middle school students
- MATh.en.JEANS' congress**, Univ. Lyon 1, Lyon. **March 2018**
Invited popularisation talk for middle school students about mathematical origamis
- MFPP's National Days**, Origami and computational complexity, Blois. **May 2017**
Popularisation talk about the link between origami and computational complexity.
- Rencontres du troisième cycle**, É.N.S. de Lyon, With Simon Castellan. **February 2017**
10 minutes presentation of what is a PhD in Computer Science.
- APMEP's National Days**, Origami and computational complexity, Lyon. **October 2016**
Popularisation talk about the link between origami and computational complexity.
- Fête de la Science**, É.N.S. de Lyon, Lyon. **October 2016**
Popularisation talk about zero-knowledge proofs.
- Al-Kindi cryptography contest**, É.N.S. de Lyon, Lyon. **June 2016**

Overview of modern cryptography: the case of e-voting.

Recreational Mathematics Seminar, É.N.S. de Lyon/MMI. **October 2014 & March 2016**

Two popularisation talks: on *zero-knowledge proofs* and *mathematical origamis*.

Languages

French: Native

German: Basic

English: Fluent

Malagasy: Basic

Computer Skills

Use of Linux and Windows. Knowledge in Microsoft Office & \LaTeX usage. Proficient in C/C++ and OCaml. Familiar with Python/Sage, Bash scripting, gnuplot and magma CAS.

Software development

Group signatures, Implementation of our dynamic group signature scheme from pairings, in C. **2018**

<https://gforge.inria.fr/projects/sigmasig-c>

Discrete logarithm in small characteristic, Implementation of Granger, Kleinjung and Zumbrägel's approach, in Magma. **2014**

Barra, GPU Tesla architecture emulator, in C++. **2013**

<https://raweb.inria.fr/rapportsactivite/RA2014/alf/uid43.html>

Interests

Paper folder, table tennis player, and also popularisation on Wikipedia.

Origami

Vice-President of the MFPP, Paris. **2017-now**

Vice-President of the French Origami Association

Fabrice Mouhartem. Flying duck. In *Origami du vivant. Pliages du monde qui bouge, nage ou vole*. Vol. 2. pp. 13–14. Ed. M. Lucas. ISBN: 978-2-9556489-1-9